THE UNIVERSITY OF WATERLOO
Faculty of Mathematics

Decentralization of the Internet

Palomino Inc.
Toronto, Ontario

Prepared By
Rohit Kaushik
3A Computer Science
ID: 20755173
July 28 2021

Memorandum

To: Michelle Forrest

From: Rohit Kaushik

Date: July 28, 2021

Re: Work Report: Decentralization of the Internet

I have prepared the enclosed report on “Decentralization of the Internet”. This report, the third of four work reports that the Co-operative Education Program requires that I successfully complete as part of my BCS Co-op degree requirements, has not received academic credit yet.

The world wide web was created as a resource that would be available to everyone in the world, offering information, entertainment, and education at minimal cost. Today, the internet remains “public” and not controlled by any singular body. However, it is narrower; time is concentrated on doing a few things like checking social media and Netflix, which restrict the overall experience of the web. Any of the tech giants like Facebook, Netflix, etc. could monopolize over the time that people spend on the web, which is very similar to controlling the internet itself. This report outlines the challenges and prospects of decentralizing the internet through a novel technology – blockchain.

The Faculty of Mathematics requests that you evaluate this report for command of topic and technical content/analysis. Following your assessment, the report, together with your evaluation, will be submitted to the Math Undergrad Office for evaluation on campus by qualified work report markers. The combined marks determine whether the report will receive credit and whether it will be considered for an award.

Thank you for your assistance in preparing this report.

TABLE OF CONTENTS

LIST OF FIGURES

Executive Summary

This report on “Decentralization of the Internet” introduces the notion of an internet that is not centralized or monopolized in any manner that it is today, using a new technology called Blockchain. It first describes the current centralized architecture and points out some limitations of the same, while suggesting methods of improvement like a distributed system.

Blockchain technology is based on a consensus algorithm used between nodes in the chain to validate transactions. They are only validated if the nodes “trust” each other – a subjective word that bolsters the complex limitations of Blockchain. The benefits provided by Blockchain are apparent in the way it is used in currencies like Bitcoin and Ethereum today. It has several components which include distributed ledgers to note transactions, immutability which ensures static node values (unless a transaction occurs), and the consensus algorithm that validates these transactions, or validates mutability of nodes. Many kinds of Blockchain networks exist today, however, they all fall into one of three categories – public, consortium or private, with consortium being a hybrid of the other two. These names indicate the kinds of node permissions that are acceptable for participation in validation. The report then investigates the limitations of modern Blockchain including security, performance, selfish mining, and poor scalability. It also discusses how new, third-party technology can be integrated using this idea to improve the notion of a decentralized network.

The report concludes by summarizing the analysis and urging researchers to look into technologies like IoT and Graphchain to improve their chances of successfully integrating into Blockchain.

1.0 Introduction

The current internet is mainly centralized due to the architecture that was used in developing the routes that a user must pass through before interacting on the internet. The users pass through a singular point, which can vary in forms like the DNS (Domain Name System) which translates IP addresses between human and computer readable forms, or the ISPs (Internet Service Providers) with whom users need to establish a connection before using the internet. In the former case, the DNS creation and maintenance are monitored mainly by the Internet Corporation for Assigned Names and Numbers (Wang et al, 2017) demonstrating the monopolization. In case of the latter, ISPs control internet traffic and can allow third party influencers to access the net.

Therefore, looking to decentralize the internet is not something unusual for researchers to do. However, the transition comes with its own challenges. The foundation of the World Wide Web is based on communication through protocols such as the TCP/IP (Transfer Control Protocol/Internet Protocol) which enables the Hyper Text Transfer Protocol (Rexford et al, 2019). However, Blockchain uses its own protocols for communication, unlike HTTPS' multi-handshake protocols (Kohlweiss et al, 2015) which necessitate the establishment of communication between Blockchain and HTTPS itself.

The original architecture of the internet using HTTP was designed to be decentralized (Simperl et al, 2017). However, in the duration of its existence, it has developed into a centralized architecture.

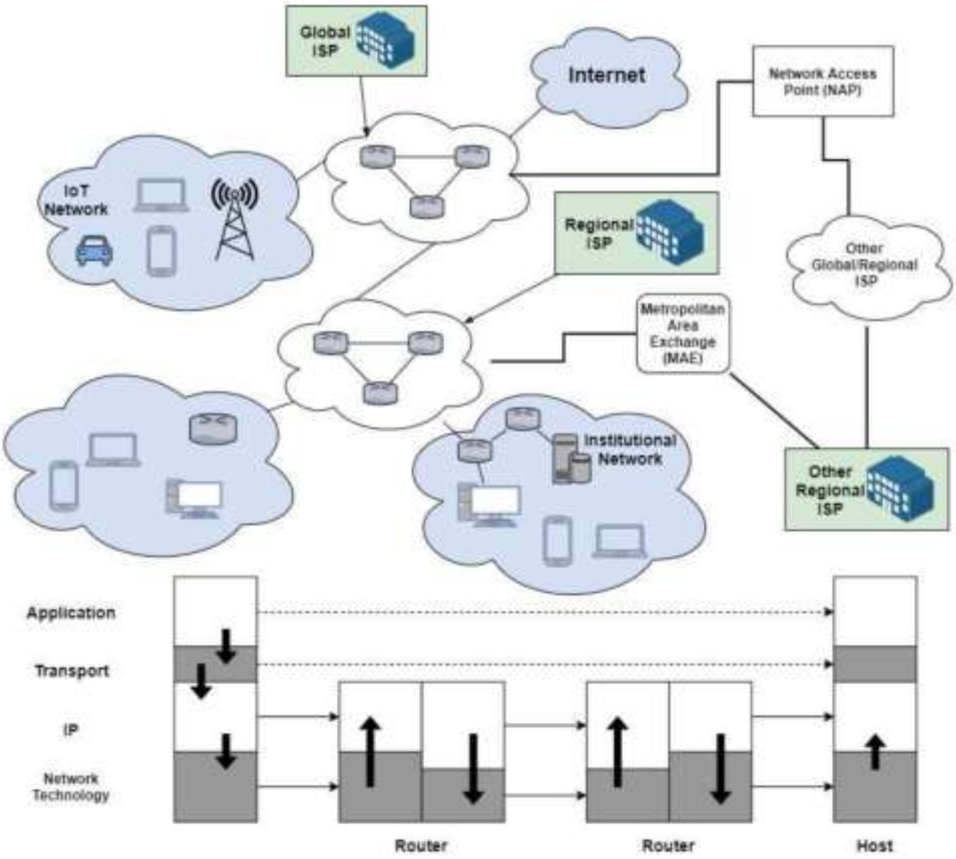


Fig. 1 – Internet Architecture

A decentralized internet would give higher data resiliency as well as improve security which encourages users to co-operate on the project and expand it (Cho et al, 2019). Successful examples of decentralized Internet can be seen on projects like The Onion Route (TOR), Zeronet, and The Invisible Internet Project (I2P), which aim to allow users to surf the web anonymously with a reduced footprint. There are two researched ways to achieve decentralization of the web. The first creates a purely decentralized network which relies on "trust" among anonymous users to ensure control is from many users and not a centralized point. This method, however, would render many newer features of the internet useless. The second method is a distributed network which asks computers on a network to be co-related and interconnected to each other. This would allow the current centralized systems to continue running on the network in a decentralized fashion.

2.0 Analysis

Blockchain allows the internet to achieve a distributed state by allowing “trust” to be shared across various networks within the overall internet structure. This gives us the notion of a network of trusts that are shared between various nodes in the blockchain network. In many of the decentralized projects that have been realised so far, Peer-to-Peer (P2P), data storage and encryption play an essential role in each project. Since these traits are inherent to Blockchain, it is a viable technology for decentralization of internet. The figure below outlines how this is achieved.

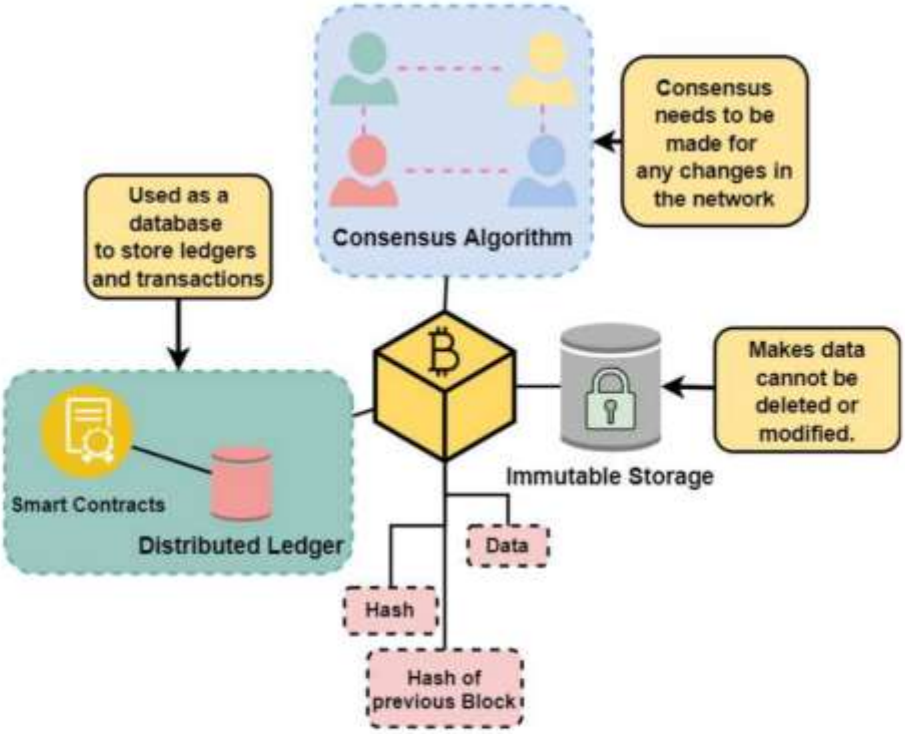

Consensus needs to be made for any changes in the network
Consensus Algorithm
Used as a database to store ledgers and transactions
Makes data cannot be deleted or modified.
Immutable Storage
Smart Contracts
Distributed Ledger
Data
Hash
Hash of previous Block

Fig. 2 – Blockchain Technology

2.1 What is Blockchain?

Blockchain is used in this context as a database used to store a decentralized network (Pierro, 2017). It is commonly used today as forms of cryptocurrency like Bitcoin, Ethereum, and more. However, this is not the technology's only possible utility. Asymmetric cryptography combined with a distributed consensus algorithm together help provide user security in Blockchain (Zheng et al, 2017). As seen below, the financial Blockchain process begins with a transaction request, which is stored in a block. This block is then propagated throughout the Blockchain network for validation. Upon verification, it will be successfully inserted at the end of the block chain (the chain that forms the network) to finish the transaction.

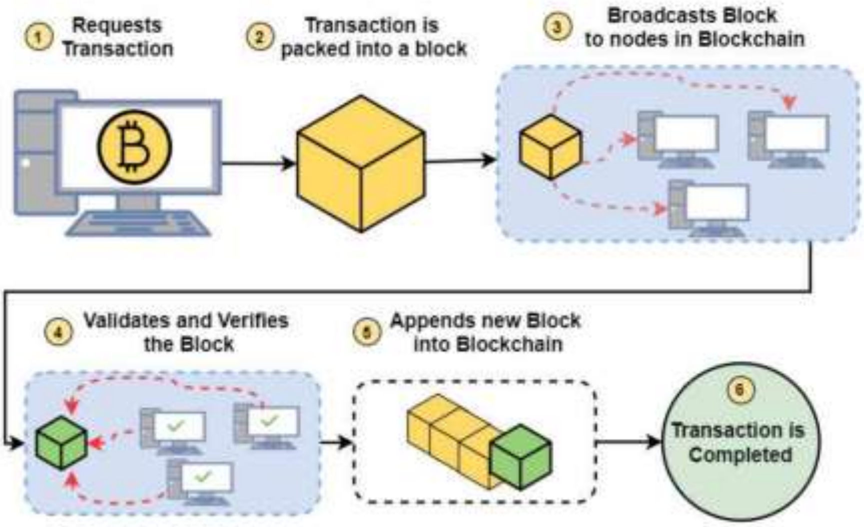

1 Requests Transaction
2 Transaction is packed into a block
3 Broadcasts Block to nodes in Blockchain
4 Validates and Verifies the Block
5 Appends new Block into Blockchain
6 Transaction is Completed

Fig. 3 – Blockchain Process for Transactions

Blockchain has various characteristics:

1. Decentralization – transactions occur using a consensus algorithm between two nodes only to prevent central authority.
2. Persistency – transactions musted be validated by trusted parties and miners.

3. Anonymity – each miner has a uniquely generated ID to remain anonymous to each other.
4. Auditability – a characterization of verification and trackability of transactions (Zheng et al, 2017).

2.2 Sub-components of Blockchain

There are three components that constitute and support Blockchain:

1. Distributed Ledgers:

   A distributed database that forms a network connection between users (or nodes). Ledgers are present as a transaction record within every node along with timestamps (Halaburda, 2018). These can only be appended within the database, ensuring security. Initially, it was done through P2P, followed by Smart Contracts – which are software that control transmission of ledgers between nodes (Subea et al, 2018).

2. Immutable Storage:

   The nodes cannot be altered once they are formed. The databases are stored in each node and has a self-referential pointer in the Blockchain as immutable evidence of the existence of a transaction (Elsden et al, 2018). This helps maintain integrity of legers in the nodes by ensuring no other means of alteration of nodes except for another valid transaction occurring.

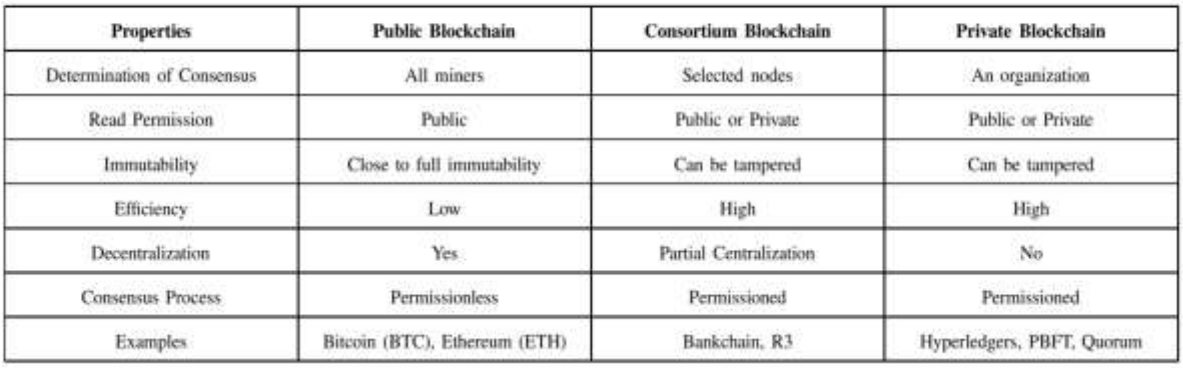
3. Consensus Algorithm:

   An algorithm intended for nodes to achieve consensus in order to validate and verify a transaction which alters the ledgers, appending them to end of the Blockchain as a new node (Magnusson et al, 2019).

2.3 Types of Blockchain

There are three categories of Blockchain as shown in Fig. 4 below (Gervais et al, 2018):

1. *Public* Blockchain is open to everybody to participate in the consensus and verification process. Nodes have full readability and writability. Examples include Bitcoin and Ethereum. Cryptocurrency has an open source development policy.
2. *Consortium* Blockchain uses an algorithm to select a random user (node) from either the public or private branch of the Blockchain to participate in verification. It is a hybrid between public and private blockchains. Examples are seen in finance like IBM/Maersk or in health with Hashed Health.
3. *Private* Blockchain uses nodes from an organization or group that is restricted from the public for validation of transactions. Not every node can participate in both processes even if they are from the same group. The selection algorithm is permissioned. Examples include Hyperledgers and Corda.



Properties	Public Blockchain	Consortium Blockchain	Private Blockchain
Determination of Consensus	All miners	Selected nodes	An organization
Read Permission	Public	Public or Private	Public or Private
Immutability	Close to full immutability	Can be tampered	Can be tampered
Efficiency	Low	High	High
Decentralization	Yes	Partial Centralization	No
Consensus Process	Permissionless	Permissioned	Permissioned
Examples	Bitcoin (BTC), Ethereum (ETH)	Bankchain, R3	Hyperledgers, PBFT, Quorum

Fig. 4 – Types of Blockchain

Broadly, Blockchains can be divided into two categories. The permissive type allows open participation in consensus using a P2P method. This uses distributed networks with trusted third-party mediators for validation procedure.

The permissioned system uses selection to pick nodes for the validation process. There is an issue regarding the trustworthiness of the chosen nodes in the validation process. However, a permissionless Blockchain would create a lawless environment where consensus can be monopolized by votes (Lopez et al, 2019).

2.4 Limitations of Blockchain

Today, Blockchain is considered to be partially decentralized (Pierro et al, 2017). There is a slight centralization of nodes which presents its own challenges. These include:

1. Scalability: Each transaction is needed to be verified by a single central node, which would lead to bottlenecks and queues in case of a large volume of simultaneous transactions. This is especially common in multichain Blockchains which use one node to validate transactions on two or more chains parallelly (Kang et al, 2019).
2. Performance: Current performance of Blockchain systems has issues that impede it and make it slower. Smart Contracts has an issue of inefficient transmission between nodes, as well as forking where one block is being mined by multiple nodes (Damsgaard et al, 2019).
3. Privacy: There have been some situations where the security and anonymity of both nodes involved in the validation process have been compromised (Sayadi et al, 2018). Information from the primary keys of the nodes can be extracted which could expose the users' transactions. From this, nodes can be mutated which disrupt the entire Blockchain and corrupt it (Florian et al, 2019).
4. Mining: Miners with ulterior motives could try to store the mined blocks and retain them until their conditions have been met. This creates a paucity of resources for

regular miners. Personalization mining is also an issue wherein it becomes difficult to specify Blockchains to interact with internet services like APIs. This could be mitigated using AI to make parts of Blockchains smarter (Florian et al, 2019).

2.5 New Technologies

Various technologies that have arisen have potential to be integrated into Blockchain, creating new opportunities regularly that can help further Blockchain technology. This is very similar to how the internet itself was developed. IoT could impact Blockchain by way of every hardware connected to the internet functioning as a node. Graphchain is a developing technology that build on and expands Blockchain.

1. Internet of Things (IoT)

   IoT has made it possible for internet connectivity to be pushed to smart devices. This caused a massive centralization of devices itself, since the internet is very much centralized (Gomathi et al, 2018). With the increase in number of smart devices replacing desktops, it is possible to integrate these devices as decentral nodes in a Blockchain network. However, further research is needed to do this since the problem of communication between different types of smart devices remains unsolved.

2. Graphchain

   Graphchain replaces Blockchain' linearly linked network structure with a graph of nodes. This becomes a decentralized graph of self-scaling and self-regulated cross-verifying transaction framework (Boyen et al, 2018). Graphchain disseminates the transaction data in "data shards" between multiple nodes in the graph chain, improving scalability. It also uses parallel mining (Kan et al, 2018).

Despite the potential Graphchain depicts, it suffers from the foundational problem of centralization, a minor issue in this case, where the central node is a common descendent of multiple nodes that are created from it (Kan et al, 2018).

3.0 Conclusion

The report begins with an introduction to the architecture of the internet, explaining its centralized structure at the moment due to the existence of DNS and ISPs. The path to decentralization has its impedances in the form of different technologies using different protocols. The internet uses HTTP while Blockchain uses completely different ones. The report then introduces the concept of “trust” among nodes in the Blockchain system as being one of the founding principles of building a decentralized internet. This is the underlying principle of consensus algorithms that Blockchain uses to validate transactions. The report then goes on to analyse Blockchain in greater detail. It first looks into the consensus algorithm as a trust system between networks within a Blockchain that utilizes nodes in either a permissionless or a permissioned manner. It defines Blockchain to be a decentralized database stored in nodes to track transactions and describes the process of appending a new block to the chain using a validation system between nodes that “trust” each other. The characteristics of Blockchains include decentralization, persistency, anonymity, and auditability. The components of Blockchain are the consensus algorithm for validation, distributed ledgers inside nodes and the immutability of nodes that ensure security to users’ data and transaction history. The report then compares the types of Blockchain networks like public, consortium (hybrid), and private.

It further discusses the limitations of Blockchain which include centralization during scaling, slow performance rate of current technology, security issues and selfish mining.

Finally, the report investigates new technologies that can overcome these limitations of the current Blockchain – third party technologies like IoT and Graphchain have the potential to propel Blockchain-based Internet systems. It also discusses their current limitations due to a paucity of research and encourages further research into these topics for the betterment of Blockchain.

Acknowledgements

This report was inspired by a curiosity I had toward cryptocurrency; reading about this led me to the usage of Blockchain not only as a currency but as a tool to restructure the entire World Wide Web. I wondered how this could be done and to what extent it has already been achieved, while also thinking about meaningful limitations that need to be overcome through further thorough research. This report was created using a plethora of research papers from the IEEE International Congress and the ACM meetings, among other sources.

References

1. *X. Wang, K. Li, H. Li, Y. Li, and Z. Liang. "Consortiumdns: A distributed domain name service based on consortium chain." IEEE 19th International Conference on High Performance Computing and Communications; pages 617–620, 2017.*

   From: https://arxiv.org/pdf/2011.01096.pdf

2. *P. Zave, and J. Rexford. "The compositional architecture of the internet." Commun.ACM, 62(3):78–87, 2019.*

   From: https://arxiv.org/pdf/2011.01096.pdf

3. *M. Kohlweiss, U. Maurer, C. Onete, B. Tackmann, and D. Venturi. "De-constructing tls 1.3. In Proceedings of the 16th International Conference on Progress in Cryptology", 2015.*

   From: https://dl.acm.org/doi/proceedings/10.5555/2985797

4. *L. Ib´a ˜nez, E. Simperl, F. Gandon, and H. Story. "Redecentralizing the web with distributed ledgers," 2017.*

   From: https://ieeexplore.ieee.org/document/7851141

5. *S. Cho and S. Lee. "Survey on the application of blockchain to iot. In 2019 International Conference on Electronics, Information, and Communication (ICEIC)," Jan 2019.*

   From: https://ieeexplore.ieee.org/document/8706369

6. *M. D. Pierro. "What is the blockchain?" 2017.*

   From: https://cse.sc.edu/~mgv/csce190f18/diPierro_mcs2017050092.pdf

7. *Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. "An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data." 2017.*

   From: https://arxiv.org/pdf/2011.01096.pdf

8. *H. Halaburda. "Blockchain revolution without the blockchain?" Commun.ACM, 2018.*

   From: https://www.bankofcanada.ca/wp-content/uploads/2018/03/san2018-5.pdf

9. G. Suciu, C. Nˇadrag, C. Istrate, A. Vulpe, M. Ditu, and O. Subea. “Comparative analysis of distributed ledger technologies.” Global Wireless Summit (GWS), 2018.
From: https://ieeexplore.ieee.org/document/8686563

10. C. Elsden, B. Nissen, K. Jabbar, R. Talhouk, C. Lustig, P. Dunphy, C. Speed, and J. Vines. “Hci for blockchain: Studying, designing, critiquing and envisioning distributed ledger technologies.” In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, 2018.
From:https://www.researchgate.net/publication/324660824_HCI_for_Blockchain_Studying_Designing_Critiquing_and_Envisioning_Distributed_Ledger_Technologies

11. A. G. Labouseur, M. Johnson, and T. Magnusson. “Demystifying blockchain by teaching it in computer science: Adventures in essence, accidents, and data structures.” 2019.
From: https://dl.acm.org/doi/10.5555/3344051.3344055

12. K. W¨ust and A. Gervais. “Do you need a blockchain?” In 2018 Crypto Valley Conference on Blockchain Technology, 2018.
From: https://arxiv.org/pdf/2011.01096.pdf

13. P. G. Lopez, A. Montresor, and A. Datta. “Please, do not decentralize the internet with (permissionless) blockchains!” In 2019 IEEE 39th International Conference on Distributed Computing Systems, 2019.
From: https://arxiv.org/abs/1904.13093

14. W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang. “A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future,” 2019.
From: https://ieeexplore.ieee.org/document/8717702

15. F. J. Couto da Silva, S. B. Damsgaard, M. A. Mousing Sorensen, F. Marty, B. Altariqi, E. Chatzigianni, T. K. Madsen, and H. P. Schwefel. “Analysis of blockchain forking on an ethereum network”, 2019.
From: https://arxiv.org/pdf/2011.01096.pdf

16. *S. Sayadi, S. B. Rejeb, and Z. Choukair. "Blockchain challenges and security schemes: A survey. In 2018 Seventh International Conference on Communications and Networking," 2018.*
    From: https://ieeexplore.ieee.org/document/8621944
17. *M. Florian, S. Henningsen, S. Beaucamp, and B. Scheuermann. "Erasing data from blockchain nodes." 2019.*
    From: https://www.semion.io/doc/erasing-data-from-blockchain-nodes
18. *R. M. Gomathi, G. H. S. Krishna, E. Brumancia, and Y. M. Dhas. "A survey on iot technologies, evolution and architecture." 2018.*
    From: https://arxiv.org/pdf/2011.01096.pdf
19. *X. Boyen, C. Carr, and T. Haines." Graphchain: A blockchain-free scalable decentralised ledger". In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, 2018.*
    From: https://ieeexplore.ieee.org/document/8452820
20. *J. Kan, S. Chen, and X. Huang "Networking. Improve blockchain performance using graph data structure and parallel mining." In 2018 1st IEEE International Conference, 2018.*
    From: https://arxiv.org/abs/1808.10810

Image Sources

1. *Fig. 1 - https://arxiv.org/pdf/2011.01096.pdf*
2. *Fig. 2 - https://arxiv.org/pdf/2011.01096.pdf*
3. *Fig. 3 - https://arxiv.org/pdf/2011.01096.pdf*
4. *Fig. 4 - https://arxiv.org/pdf/2011.01096.pdf*